Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1 (original): A system for actively updating a cryptography module in a security gateway, the security gateway connected between a user computer system and a network system, the system comprising:

a Web GUI for generating at least one window in the user computer system, the window having a decryption/encryption module update system to allow a user to upload a new decryption/encryption module to the security gateway by the Web GUI;

an extended library for accommodating a decryption/encryption module; and

a module update unit for actively updating a corresponding decryption/encryption module in the extended library according to the new decryption/encryption module uploaded to the security gateway or adding the uploaded decryption/encryption module into the extended library.

2 (original): The system of claim 1 wherein the security gateway is a VPN gateway complying with an IPSEC protocol.

3 (original): The system of claim 1 wherein the security gateway includes a current library, a kernel, and a daemon, the module update unit being located in the current library.

4 (original): The system of claim 1 wherein the decryption/encryption module update system in the window of the Web GUI includes a system for allowing the user to update a current decryption/encryption module

in the security gateway.

5 (original): The system of claim 4 wherein the decryption/encryption module update system in the window of the Web GUI further includes a defined decryption/encryption module system for allowing the user to add a defined decryption/encryption module into the security gateway.

6 (original): The system of claim 5 further comprising a defined module unit connected to the defined decryption/encryption module system for generating a window for providing the user with an instruction to fill in a field in the window with a description of the defined decryption/encryption module.

7 (original): The system of claim 6 wherein the description of the defined decryption/encryption module includes an algorithm, algorithmic identifier, data encryption block size, key length, and decryption/encryption executing function, the parameters of the decryption/encryption executing function including a data address, data block size, key information, key length, initial vector, and decryption/encryption flag.

8 (original): The system of claim 1 wherein the module update unit selects to actively update the corresponding decryption/encryption module in the extended library or to add the uploaded decryption/encryption module into the extended library according to the new decryption/encryption module.

9 (original): The system of claim 2 further comprising an extended library interface for assisting the extended library to communicate with the current library and the kernel.

10 (original): The system of claim 1 further comprising a configuration set unit such as a system file for setting an execution process according to an IPSEC protocol wherein after a decryption/encryption module is updated or added, the key exchange process is updated according to an IKE protocol.

11 (original): A method for actively updating a cryptography module in a security gateway, the security gateway connected between a user computer system and a network system, the method comprising:

downloading a new decryption/encryption module to the user computer system through the network system;

starting a Web GUI of the security gateway for generating at least one window in the user computer system, the window having a decryption/encryption module update system;

selecting a decryption/encryption module from the window provided by the Web GUI;

uploading the selected decryption/encryption module to the security gateway;

a module update unit of the security gateway actively updating a corresponding decryption/encryption module in the extended library according to the uploaded decryption/encryption module or adding the uploaded decryption/encryption module into the extended library; and

updating a key exchange process in the security gateway according to an IKE protocol.

12 (original): The method of claim 11 wherein the decryption/encryption module update system in the window of the Web GUI includes a system for allowing the user to update a current

decryption/encryption module in the security gateway.

13 (original): The method of claim 12 wherein the decryption/encryption module update system in the window of the Web GUI further includes a defined decryption/encryption module system for allowing the user to add a defined decryption/encryption module into the security gateway.

14 (original): The method of claim 13 further comprising:

when starting the defined decryption/encryption module, generating a window for providing a user with an instruction to fill in a field in the window with a description of the defined decryption/encryption module.

15 15 (original): The method of claim 14 wherein the descriptions of the defined decryption/encryption module includes an algorithm, algorithmic identifier, data encryption block size, key length, and decryption/encryption executing function, the parameters of the decryption/encryption executing function including a data address, data block size, key information, key length, initial vector, and decryption/encryption flag.

16 (original): The method of claim 11 further comprising:

the security gateway executing the updated key exchange process.

17 (cancelled)